

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. (Currently amended) A method for sharing a secure communication
2 session with a client between a plurality of servers, comprising:
3 receiving a message from the client at a first server in the plurality of
4 servers, the message including a session identifier that identifies a secure
5 communication session with the client; and
6 if the session identifier does not correspond to an active secure
7 communication session on the first server, establishing an active secure
8 communication session with the client on the first server by,
9 attempting to retrieve state information associated with the
10 session identifier for an active secure communication session
11 between the client and a second server from the plurality of
12 servers, wherein the state information includes an agreed upon
13 encryption key used to encrypt communications between the client
14 and the second server,
15 if the state information for the active secure communication
16 session is retrieved, using the state information including the
17 encryption key to use an existing the active secure communication
18 ~~session for the secure communication session established~~ between
19 the client and the second server ~~so that the secure communication~~
20 is for subsequent communications between the client and the first
21 server without ~~setting~~ having to set up a new secure

22 | communication session ~~including any related cryptography between~~
23 | the client and the first server, and
24 | if the state information for the active secure communication
25 | session is not retrieved, communicating with the client to establish
26 | the active secure communication session with the client.

1 | 2. (Original) The method of claim 1, wherein attempting to retrieve the
2 | state information includes:
3 | attempting to use the session identifier to identify the second server in the
4 | plurality of servers that has an active secure communication session with the
5 | client that corresponds to the session identifier; and
6 | attempting to retrieve the state information from the second server.

1 | 3. (Original) The method of claim 1, wherein attempting to retrieve the
2 | state information involves attempting to retrieve the state information from a
3 | centralized repository that is in communication with the plurality of servers.

1 | 4. (Original) The method of claim 3, wherein the centralized repository
2 | includes a database for storing the state information.

1 | 5. (Original) The method of claim 1, wherein establishing the active
2 | secure communication session involves establishing a secure sockets layer (SSL)
3 | connection with the client.

1 | 6. (Original) The method of claim 1, wherein the state information
2 | includes:
3 | a session encryption key for the secure communication session;
4 | the session identifier for the secure communication session; and

5 a running message digest for the secure communication session.

1 7. (Original) The method of claim 6, further comprising:
2 using the message to update the running message digest; and
3 checkpointing the updated running message digest to a location outside of
4 the first server.

1 8. (Original) The method of claim 1, further comprising, if the state
2 information for the active secure communication session is retrieved, purging the
3 state information from a location from which the state information was retrieved,
4 so that the state information cannot be subsequently retrieved by another server in
5 the plurality of servers.

1 9. (Original) The method of claim 1, further comprising initially
2 establishing an active secure communication session between the client and the
3 second server, the active secure communication session being identified by the
4 session identifier.

1 10. (Original) The method of claim 1, wherein attempting to retrieve the
2 state information includes authenticating and authorizing the first server.

1 11-12 (Canceled).

1 13. (Currently amended) A computer-readable storage medium storing
2 instructions that when executed by a computer cause the computer to perform a
3 method for sharing a secure communication session with a client between a
4 plurality of servers, the method comprising:

5 receiving a message from the client at a first server in the plurality of
6 servers, the message including a session identifier that identifies a secure
7 communication session with the client; and
8 if the session identifier does not correspond to an active secure
9 communication session on the first server, establishing an active secure
10 communication session with the client on the first server by,
11 attempting to retrieve state information associated with the
12 session identifier for an active secure communication session
13 between the client and a second server from the plurality of
14 servers, wherein the state information includes an agreed upon
15 encryption key used to encrypt communications between the client
16 and the second server,
17 if the state information for the active secure communication
18 session is retrieved, using the state information including the
19 encryption key to use ~~an existing~~ the active secure communication
20 ~~session for the secure communication session established~~ between
21 the client and the second server ~~so that the secure communication~~
22 ~~is for subsequent communications between the client and the first~~
23 ~~server without setting having to set up a new secure~~
24 ~~communication session including any related cryptography between~~
25 the client and the first server, and
26 if the state information for the active secure communication
27 session is not retrieved, communicating with the client to establish
28 the active secure communication session with the client.

1 14. (Original) The computer-readable storage medium of claim 13,
2 wherein attempting to retrieve the state information includes:

3 attempting to use the session identifier to identify the second server in the
4 plurality of servers that has an active secure communication session with the
5 client that corresponds to the session identifier; and
6 attempting to retrieve the state information from the second server.

1 15. (Original) The computer-readable storage medium of claim 13,
2 wherein attempting to retrieve the state information involves attempting to
3 retrieve the state information from a centralized repository that is in
4 communication with the plurality of servers.

1 16. (Original) The computer-readable storage medium of claim 15,
2 wherein the centralized repository includes a database for storing the state
3 information.

1 17. (Original) The computer-readable storage medium of claim 13,
2 wherein establishing the active secure communication session involves
3 establishing a secure sockets layer (SSL) connection with the client.

1 18. (Original) The computer-readable storage medium of claim 13,
2 wherein the state information includes:
3 a session encryption key for the secure communication session;
4 the session identifier for the secure communication session; and
5 a running message digest for the secure communication session.

1 19. (Original) The computer-readable storage medium of claim 18,
2 wherein the method further comprises:
3 using the message to update the running message digest; and

4 checkpointing the updated running message digest to a location outside of
5 the first server.

1 20. (Original) The computer-readable storage medium of claim 13,
2 wherein the method further comprises, if the state information for the active
3 secure communication session is retrieved, purging the state information from a
4 location from which the state information was retrieved, so that the state
5 information cannot be subsequently retrieved by another server in the plurality of
6 servers.

1 21. (Original) The computer-readable storage medium of claim 13,
2 wherein the method further comprises initially establishing an active secure
3 communication session between the client and the second server, the active secure
4 communication session being identified by the session identifier.

1 22. (Original) The computer-readable storage medium of claim 13,
2 wherein attempting to retrieve the state information includes authenticating and
3 authorizing the first server.

1 23-24 (Canceled).

1 25. (Currently amended) An apparatus that shares a secure communication
2 session with a client between a plurality of servers, comprising:
3 a receiving mechanism, at a first server in the plurality of servers, that
4 receives a message from the client, the message including a session identifier that
5 identifies a secure communication session with the client;
6 an examination mechanism that examines the session identifier; and

7 a session initialization mechanism, on the first server, wherein if the
8 session identifier does not correspond to an active secure communication session
9 on the first server, the session initialization mechanism is configured to establish
10 an active secure communication session with the client by,
11 attempting to retrieve state information associated with the
12 session identifier for an active secure communication session
13 between the client and a second server from the plurality of
14 servers, wherein the state information includes an agreed upon
15 encryption key used to encrypt communications between the client
16 and the second server,
17 if the state information for the active secure communication
18 session is retrieved, using the state information including the
19 encryption key to use an existing the active secure communication
20 session ~~for the secure communication session established~~ between
21 the client and the second server ~~so that the secure communication~~
22 ~~is~~ for subsequent communications between the client and the first
23 server without ~~setting~~ having to set up a new secure
24 communication session ~~including any related cryptography between~~
25 the client and the first server, and
26 if the state information for the active secure communication
27 session is not retrieved, communicating with the client to establish
28 the active secure communication session with the client.

1 26. (Original) The apparatus of claim 25, wherein the session initialization
2 mechanism is configured to attempt to retrieve the state information by:
3 attempting to use the session identifier to identify the second server in the
4 plurality of servers that has an active secure communication session with the
5 client that corresponds to the session identifier; and

6 attempting to retrieve the state information from the second server.

1 27. (Original) The apparatus of claim 25, wherein the session initialization
2 mechanism is configured to attempt to retrieve the state information by attempting
3 to retrieve the state information from a centralized repository that is in
4 communication with the plurality of servers.

1 28. (Original) The apparatus of claim 27, wherein the centralized
2 repository includes a database for storing the state information.

1 29. (Original) The apparatus of claim 25, wherein the active secure
2 communication session includes a secure sockets layer (SSL) connection with the
3 client.

1 30. (Original) The apparatus of claim 25, wherein the state information
2 includes:
3 a session encryption key for the secure communication session;
4 the session identifier for the secure communication session; and
5 a running message digest for the secure communication session.

1 31. (Original) The apparatus of claim 30, further comprising an updating
2 mechanism that is configured to:
3 use the message to update the running message digest; and to
4 checkpoint the updated running message digest to a location outside of the
5 first server.

1 32. (Original) The apparatus of claim 25, further comprising a purging
2 mechanism that is configured to purge the state information from a location from

3 which the state information was retrieved, so that the state information cannot be
4 subsequently retrieved by another server in the plurality of servers.

1 33. (Original) The apparatus of claim 25, wherein the session initialization
2 mechanism is configured to authenticate and authorize the first server prior to
3 receiving the state information.

1 34-35 (Canceled).